Privacy Issues Involved in Electronic Government

Prepared for the Electronic Government Task Force: Strategic Issues Subcommittee
By the Department of Information Resources

August 2000
Austin, Texas

"I'm a privacy-rights person. The marketplace can function without sacrificing the privacy of individuals.
-- Texas Governor George W. Bush[1]

Executive Summary

Privacy is the greatest hindrance to successful online government. Numerous surveys and reports have found that consumers and citizens feel that lack of privacy protection to be the number one deterrent for conducting online transactions. Texas Online will have to overcome this general distrust of online transactions and convince users that Texas e-government respects their personal privacy.

Like many states, Texas does not have a comprehensive privacy law. Instead, Texas has a patchwork of 580 statutes that protect specific personal information in limited circumstances. In addition, the Public Information Act, the act that governs information management in Texas, does not do enough to protect the personal information of the average citizen in the State of Texas. It is imperative that Texas pass privacy legislation for the success of Texas Online and future state online endeavors. Such legislation needs to address the following considerations:

First, the Public Information Act of 1973 offers little privacy protection for the average citizen in Texas. Even under the conditions of its broadest exception, the common law tort, very little data collected by the State is protected from public disclosure. Consequently, the selling of Texans' personal information obtained by Texas State government is becoming a profitable business. Recent public surveys have found the public concerned and surprised that the state distributes and sells their personal information. The Public Information Act must be revised in order to provide the privacy protection that citizens expect as they visit the State portal, Texas Online.

Second, current data management policies in state agencies undermine the state privacy laws currently in place. For example, state laws protecting information held by one state agency can be accessed by another state agency. The home address and telephone number of a Texas governmental employee is protected by the Public Information Act only if the employee opts out, but this same information can be obtained if the employee obtains a fishing license from the Texas Parks and Wildlife Department. Another example of the undermining of state privacy laws concerns the lack of technology. For instance, some agencies do not have the technology to electronically scramble or redact confidential information contained in a database before issuing it to an open records requestor. Consequently, information deemed confidential is being distributed to the public. Lastly, some agencies may be collecting data without any deliberation on the necessity of the data in providing service to the citizen. Therefore, any information held by that agency can be accessed through legitimate open records requests and by cracks in the system, as described above. If action is not taken, Texas state government will experience a backlash from the public as it discovers that its information is not protected across state agencies and that strict records management procedures are either not established or not adhered to. Paying special attention to the administrative execution of privacy and data protection laws will further protect citizens' personal information from undue public disclosure.

Third, many countries are successfully protecting the privacy of their citizens through the adoption of a privacy law and the establishment of a privacy commission to enforce the law. The establishment of a privacy commission would be a significant step to protecting online and offline privacy of Texans on a full-time basis.

The following recommendations will move Texas towards the protection of its citizens' personal privacy and increase the public's trust in Texas Online. Please note that each of the possible solutions is prefaced by a code that directs the reader to the specific government body the recommendation most concerns:

- *LEG* – These are recommendations that require legislative action in order to be implemented.
- *STATE* – These are recommendations that can be implemented by state agency action.
- *TF* – Task Force initiatives may require setting portal policies and standards.

[1] Walczak, Lee. Edited. "Surprise! Bush is Emerging as a Fighter for Privacy on the Net." Business Week. 5 June 2000.

1. (LEG/STATE) State agencies should be very deliberate about every piece of data collected on individuals, and collect only that data for which there is a legitimate governmental need as determined by the agency's board.

2. (LEG) Citizens should have the right to review and challenge the accuracy of the information collected and held about them through the State portal. ..

3. (STATE) Citizens should be provided clear and complete information about the privacy policies under which state agencies operate. Privacy policies should avoid "legalese" and should describe why and how personal information is collected and how it is used.

4. (STATE) Agencies must be held accountable for faithfully executing their privacy policies and the law. This includes having strong security measures in place to safeguard private information against unauthorized intrusions and coordinate efforts with authorized third parties to perform unannounced annual checks of portal participating governmental agencies to ensure that privacy policies are being adhered to.

5. (LEG) The Legislature should establish a privacy commission that is authorized to do the following:

    - Investigate complaints and assist government agencies routinely in complying with applicable privacy rules and statutes;
    - Educate the public on how to protect their privacy and how to access public information from state government;
    - Provide a Privacy Hotline where individuals and government agencies can get general information and advice concerning their privacy rights under Texas law;
    - Conduct policy analysis on proposed and existing legislation in concert with the Office of the Attorney General for privacy implications and conduct research into technological and social developments that can affect personal privacy;
    - Meet with records management and online privacy personnel in each agency annually to identify and address privacy concerns of agencies and to determine compliance with the Public Information Act and potential privacy act(s).

The State of Texas must act now to protect citizen privacy. Privacy is not an issue that can be overlooked in government's effort to serve the public through online means. Once personally identifiable data is released, there is no way to determine who has access to the data and the purposes the data is used. Recent studies and surveys suggest that the public is concerned about who has personal information about them and what that information is being used for. By implementing these recommendations, Texas State government will be taking the first steps in ensuring privacy of personal information given through the State portal, raising the public's comfort level, and increasing the use of government services online.

Background

Recognizing the importance of electronic commerce to the state and its potential to help increase the effectiveness of state government, the Texas State Legislature mandated the demonstration of electronic government through Senate Bill 974 (Section 2054.062). The 1999 legislation charges the Department of Information Resources with "establishing a task force to assess the current and future feasibility of establishing a common electronic system using the Internet through which state agencies and local governments can accomplish the following types of functions electronically:

1. Send documents to members of the public and persons who are regulated by a state agency or local government;
2. Receive applications for licenses and permits and receive documents for filing from members of the public and persons who are regulated by a state agency or local government that, when a signature is necessary, can be electronically signed by the member of the public or regulated person; and
3. Receive required payments from members of the public and persons who are regulated by a state agency or local government."

The Task Force is composed of a representative of each of the following state officers or agencies:

- the Department of Information Resources;
- the Office of the Secretary of State;
- the Office of the Comptroller of Public Accounts;
- the Texas Department of Economic Development;
- the General Services Commission;
- the Texas Natural Resource Conservation Commission;
- the Texas Department of Insurance;
- the Public Utility Commission of Texas; and
- representatives of local governments appointed by the governor in the number determined by the governor;
- three representatives of businesses that are regulated by a state agency or local government, appointed by the governor; and
- three public members appointed by the governor.

To accomplish its mission, the Task Force elected to issue a statewide contract for development of a "common business portal" as a framework through which members of the public and persons who are regulated by a state agency or local government can do the following:

- send documents to members of the public and persons who are regulated by a state agency or local government;
- receive applications for licenses and permits;
- receive documents for filing; and
- receive required payments.

This report was written to provide the Texas Legislature an overview of the issues surrounding privacy on the Internet, and tension between providing open, transparent government, and the need to protect sensitive personal information of citizens.
Lastly, the report offers policy recommendations concerning the privacy policies of the State portal and legislation needed to protect citizen information transmitted through the portal.

The report is divided into four major topic areas:

- Privacy in Texas
- Government Reactions to Citizen Concern
- Privacy Commission
- Recommendations

"The makers of our Constitution...sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred as against the Government, the right to be let alone -- the most comprehensive of the rights of man and the right most valued by civilized men."
-- U.S. Supreme Court Justice Louis D. Brandeis, dissenting in Olmstead v. United States (1928)

Introduction

Since 1973, Texas has had an Open Records policy. The Public Information Act was passed in an effort to make State government more transparent and accountable to the people. The Act makes most recorded information collected and maintained by the State public information. Although Texas citizens are given the right to access a wealth of "public information," much of this information was often difficult to obtain. Traditionally, documents were filed away in warehouses or buried in file cabinets. With the advent of the Internet, access to public information is becoming increasingly easy. While fast and easy access is convenient, problems arise when personal information of citizens is sold and distributed.

Privacy is becoming a growing concern to consumers and citizens. In May 2000, the Federal Trade Commission released a report overturning their previous stance of self-regulation of privacy within the Internet industry. This recent action emphasizes the importance of protecting one's personal information from illegitimate forms of use without one's knowledge. The uniqueness of data is that unlike a physical object, data can be sold and distributed with relative ease in today's electronic society. The ramifications of having widespread knowledge of data are immense. One's medical and financial records could be used in hiring decisions. Social security numbers could be used in crimes of identity theft and financial fraud. Something as public as one's address could be used to conduct a hate crime. In some cases, terrorists and anti-government groups can use government security information that is deemed "public" to attack nuclear plants and other government targets.

Government is at a crossroads in dealing with the tension between open government and personal privacy. Citizens expect government to be open and accountable to the people. At the same time, citizens are growing increasingly concerned with the government selling and distributing their personal information. Such distribution is made possible, in part, by open government. Although the issue of privacy is complex, governments essentially have two broad options:

- Establish privacy policies and laws that make specified categories of personally identifiable information unavailable to the public, or
- Evaluate information on a case by case basis and preclude disclosure only when the risk of disclosure is found to be greater than the value of openness.

It is imperative that actions by government, especially Texas State government, protect citizens' right to personal privacy. Once information is released, there is no means to protect it in the future. Released information can be bought, sold, and dispersed to a variety of parties without knowing exactly who holds the information and how they are using it. At the same time, in an effort to protect the individual's right to privacy, any revision of the Public Information Act must ensure that non-confidential information is accessible for fair and equitable use.

Privacy in Texas

According to Privacy Journal, Texas ranks in the bottom tier of states when it comes to protecting citizen and consumer privacy. Robert Ellis Smith, a journalist and lawyer with the Privacy Journal, stated "We could find no (privacy) protections at all in Texas."[1] While Privacy Journal could not find any privacy protections, Texas does have over 580 separate statutes that protect personal privacy in a piecemeal fashion. These privacy protections address certain types of information in specific situations. Texas does not have a comprehensive privacy law.

Public Information Act

The key to understanding the lack of privacy in Texas' public sector rests on understanding the Public Information Act. All information held by Texas State agencies are governed by the Public Information Act. Texas adopted the Public Information Act originally in 1973 as the Texas Open Records Act in an effort to make State government more open and accountable to the people. With only thirty-five exceptions, the Act makes all information collected and maintained by the State available to the public.

Fifteen of the thirty-five exceptions deal with the protection of personal information, yet the information that is protected from disclosure is specific to a particular population and circumstance. For instance, personal information is protected for State employees, crime victims, and prison inmates; specific types of records such as, student records and library records are also protected under the exceptions to the Act. The Act does not address the privacy of the average citizen in all situations. Even the broadest exception to the Act, the common law tort, offers very little privacy protection. In order for information to be protected under common law it must be of "(1) highly intimate or embarrassing facts about a person's private affairs such that its release would be highly objectionable to a reasonable person and (2) be of no legitimate concern to the public."[2] Under the interpretations of the Office of the Attorney General, very little data that is collected by the State is of no legitimate concern to the public. Furthermore, even when the legislature attempts to make information confidential by statute, the Attorney General has declared that the statute must contain express language making the information confidential or state that the information shall not be released to the public.[3]

Unless protected by a federal law or one of the thirty-five exceptions of the Texas Public Information Act, Texans' home, employment, financial, and medical information held by Texas State government is open for any individual, organization, or company to acquire. Having such data open to the public is useful in conducting normal every day financial and social transactions. Legitimate businesses need data from state government to corroborate information given to them by customers and to comply with government regulations. Law enforcement relies on public record information to prevent, detect, and solve crimes. Private citizens use public records to locate missing family members and heirs to estates. Researches also use open public records to conduct studies concerning public safety, public health, crime, and an array of other subjects. Lastly, commercial users and resellers of public records often update them, correct inaccuracies and sell a revised version back to the government. They also lessen the volume of inquires that could potentially overwhelm government agencies by providing other outlets of public records access.[4]

While commercial resellers of public information may provide a service to the government, some citizens oppose the use of their personal information* for commercial profit-making purposes. In a survey commissioned by the Electronic Government Task Force and conducted by the University of Texas at Austin, over 60% of Texans find the selling of data for financing e-government objectionable. Currently, information on Texans can be found on Internet sites like www.publicdata.com and www.havenco.com. As more and more information is being collected and stored electronically, the instances of public record databases being acquired by companies and sold to the public will rise. The study speculates that citizens

* Personal information can refer to a variety of data, including but not restricted to, one's name, address, telephone number, tax history, social security number, credit card number, education, and credit history.

are unaware that the state already sells personal information gathered on residents or that people believe that such data should not be used as a means of financing government activities.[5]

Addressing the issue of data access is essential for widespread use of the Texas Online. People must be confident that the use of public records is consistent with their best interests. In addition, the public must also be able to trust that their personal information is used for legitimate purposes. The public should be able to trust that their data is not being sold or distributed without their consent. Although the State of Texas owns all data collected, assembled or maintained by a government body, the public considers such data to be theirs.[6] In order for Texas Online and future state e-government initiatives to be widely adopted, Texas state government must ensure that personal information in its possession is protected, whether it is owned by the State or by the citizen.

Data Management Issues

There are four primary data management issues facing Texas government: data collection and retention, assorted and uneven data protections, intergovernmental sharing of information, and data correction.

Data Collection and Retention

The first issue involves data collection and retention procedures of state agencies. The issue of data access can be answered by establishing data management procedures with privacy in mind. The first step in managing the public's data is reviewing what data is being collected by each agency. Is every piece of information gathered necessary for providing products or services to the public? Is the agency even authorized to collect such information? Are agency procedures compliant with the Public Information Act?

Once the data is entrusted with the state agency, how long does the data remain with the agency? Records management practices and retention schedules require the identification of confidential information and the establishment of procedures for protecting it. Strictly following the records management policies and retention schedules can be beneficial to both the citizen and the governmental body. The citizen know that his or her personal information will remain with the government for a defined period of time and then be destroyed. At the same time, the governmental body benefits as well, in that they will not be in violation of their own records management practices and will not be forced to give out information that they should not have. Information held past the retention date is still subject to distribution under the Public Information Act.

Assorted and Uneven Data Protections

The second issue facing policymakers is uneven data protections given by state agencies. State agencies must determine whether data deemed confidential by the Public Information Act are protected in existing databases. If a governmental entity is building new databases, privacy should be an important consideration. Goal three of the State Strategic Plan for Information Resources Management states that "Texas government will ensure the privacy, security, and historical integrity of the information and information resources entrusted to government by the people of Texas."[7] Ensuring the privacy and security of confidential data is essential to winning and retaining public trust. This means that when an agency hands over documents that have confidential information, they must redact data deemed confidential so that the recipient cannot read it. The agency must take similar measures when they give out entire databases in compliance with the Public Information Act. The agency must ensure that any confidential information contained in the database is electronically scrambled so that the recipient cannot read it.

Texas does not have a comprehensive privacy law and the Public Information Act does not protect personal information comprehensively. Each state agency has different restrictions concerning public disclosure of information. For example, the home address and telephone number of a Texas governmental employee is protected by the Public Information Act only if the employee opts out, but this same information can be obtained if the employee obtains a fishing license from the Texas Parks and Wildlife Department. This issue may cause the most confusion for citizens using Texas Online. Unless the legislature addresses the uneven protections granted to the public across state agencies, citizens using Texas Online will need to read and understand each privacy policy for all the different governmental entities participating in the portal. That which is deemed private and protected on one portal Web page may be considered public information

on another Web page of the portal. The lack of enforcement and penalties serves as an example of a situation that deteriorates public trust in government and a situation that would deter citizens from using Texas Online.

Intergovernmental Sharing of Information

The third issue of data management is the intergovernmental sharing of information. In order for Texas to meet its goal of delivering "seamless, integrated government services to citizens," it must be able to share information between agencies in order to eliminate duplication of effort and achieve economies of scale.[8] In the course of transferring data between governmental bodies, these agencies must also "ensure the integrity and security" of the data. This means that data protected from disclosure in one agency by the Public Information Act or other law must also be protected in the transfer process to another agency. Shared information between agencies should be equally protected from one agency to the next. It is unlikely that citizens will use Texas Online if they feel that their data is being passed around to different state agencies without standard privacy protection. To protect data across agencies may require new legislation.

Data Correction

A fourth issue involves data correction. Citizens should have the right to know what information the state has about them and the right to correct that information should there be any errors. This is based on the same premise as fair credit reporting. The Fair Credit Reporting Act of 1970 allows consumers to attain a copy of their credit reports and challenge any discrepancies. If agencies are able to share information and potentially keep one Texas database of all data, whether it is personal, financial, or medical, members of the public should be able to access their personal data at any time. With data maintained in a single database, the process of correcting data errors becomes much more cost-effective and efficient. Eventually, corrections could be done through Texas Online. The federal government has enacted legislation applicable to federal agencies, such as the Privacy Act of 1974, which gives individuals the right to access and correct information held by the federal government. But this federal act does not apply to state or local governments.

New Data Management Techniques

Washington State has created new techniques that would further protect citizen data held by the state and thereby increase trust in state-citizen interaction through their Web portal. The State of Washington's Governor's Work Group on Commercial Access to Government Electronic Records recommended the following techniques in 1997 in an effort to effectively manage data with respect to privacy:

- Make a distinction between *legitimate business use vs. prohibited commercial use* of government held information. The Work Group acknowledged that government has a duty to release information to companies for verification purposes and for legal compliance purposes on the part of the company. They also found that government-held information used for profit-making purposes should be restricted to some extent.
- Require that all state agencies allow access to public records for commercial purposes only through a *contractual agreement* between the agency and the entity requesting access. Such a contract would state the following:

    1) the information provided by the agency would only be used for the purpose approved by the agency;
    2) the entity would not distribute or publish any of the information provided by the agency, without express written consent;
    3) the agency may provide "control" or "salted" data as a portion of provided information as a means of ensuring that any personally identifiable information is used for the agreed purpose.

- Establishes strict penalties for entities that violate the terms of the public access contract, including loss of access and financial penalties (on a per record basis). For sensitive release

of information, a security deposit could be required against which financial penalties can be drawn.[9]

If Texas were to adopt some of the techniques that Washington State was exploring, the Public Information Act would have to be altered. Presently, it is against the law to ask a requestor what they intend to do with the information that they request.

Government Reaction to Consumer Concern

"Just because the state requires our information does not mean it has the right to sell it to the highest bidder."[10]
--Wisconsin State Rep. Mike Huebsch

Government is at a crossroads in dealing with the tension between open government and privacy of information. The federal and state governments around the nation have not been able to resolve the fact that laws currently on the books do not keep up with technology. Many of the laws specifically apply to paper records. In addition to the fact that the some of the privacy laws do not address new forms of technologies, the laws also are made moot by the fact that some legislation passed lacks oversight and enforcement.

Currently, many businesses and governments have an opt-out data release policy. The opt-out approach to personal privacy leaves the burden of protection on the individual. The person must inform the organization that they do not want their information shared with third parties. If the subject does not give such notice to the organization, the organization reserves the right to share and sell the subject's data.

A number of surveys, including the E-Government Services and Computer and Internet Use in Texas commissioned by the Electronic Government Task Force and conducted by the University of Texas at Austin, found that the public prefers an opt-in, rather than opt-out data release approach.[11] The Opt-in approach leaves the burden of protection on the business or governmental entity. The subject of the information must give the organization the permission to use their data for other than the original purpose. If such permission is not given, the organization cannot release the subject's data to third parties or use it for purposes other than what it was intended.

State Developments

States have been active in trying to address the privacy dilemma. According to the Privacy Journal, the top privacy protections are found in California, Connecticut, Florida, Hawaii, Illinois, Massachusetts, Minnesota, New York, Rhode Island and Wisconsin.[12] Nine states, namely California, Hawaii, Idaho, Kentucky, Massachusetts, Minnesota, New York, Ohio, and Virginia, have also enacted state privacy acts based on the provisions of the federal statute. These state privacy laws govern the collection, maintenance, use, and disclosure of "personal information" by the states and state agencies. Although they carry the name "privacy act," the federal and state privacy acts afford no greater protection against the release of confidential or private information than federal or state open records acts."[13] In addition, none of the acts – neither state nor federal – address the collection or use of "personal information" by non-governmental entities.

The following table demonstrates some of the legislation that is currently pending in states' legislatures. This is not meant to be a comprehensive list, but rather a sampling of state initiatives.

Pending State Legislation

State	Initiatives Pending
California	• Prohibits Internet service providers from disclosing personal information without permission of customers. • Creates an office of Privacy Ombudsman for investigative purposes of unlawful use of personal information.
Colorado	• Requires companies to post a privacy policy that discloses if data is being collected, how the data is used, and gives the consumer an opt-out option. • Establishes basic requirements for government agencies that collect, use, and disseminate personal information obtained by individuals.
Hawaii	• Provides safeguards against the unwarranted private commercial collection and dissemination of personal information about individuals. • Regulates the collection, use, and disclosure of personal information by private organizations.
Maryland	• Requires state entities to post privacy policies on their Web sites. • Prohibits the disclosure by sale, rental, or barter of medical records.
New York	• Establishes an opt-out system for unsolicited marketing. • Restricts collection, disclosure, and distribution of personal information acquired by an online computer services provider.
Virginia	• Limits authority of financial institutions to disclose personal information about its customers. • Directs every public body that has an Internet Web site to develop a privacy policy that is consistent with the Privacy Protection Act of 1976. • Prohibits the disclosure of social security number and other personal information.
Washington	• Prohibits the unauthorized transfer of personal information acquired by merchants. • Restricts the use of social security numbers as identification. • Gives consumers the opportunity to review and correct the accuracy of information that is shared or transferred with others.

U.S. National Legislation

The U.S. has not enacted comprehensive privacy legislation on the national level. Instead, the federal government has numerous privacy statutes that protect personal privacy in a piecemeal fashion. The Privacy Act of 1974 gives individuals the right to access and correct information held by the federal government. The act did not cover private entities and state and local governments. The rest of the privacy legislation enacted covers a particular circumstance or type of information. As industries and technologies change, some of the legislation has become ineffective. The table below is small sampling of the patchwork approach the federal government has taken to protecting personal privacy.

Selected National Privacy Legislation[14]

Legislation Name	Type of Entities Affected	Summary
Fair Credit Reporting Act of 1970	Private parties	Requires credit agencies to make their records available to the subjects of the records, provides procedures for the correcting of information, and permits disclosure to authorized parties.
Cable Communications Policy Act of 1984	Private parties	Requires cable services to inform subscribers of the nature of personally identifiable information collected and the use of such information; restricts the collection and disclosure of such information by cable services.
Electronic Communication Privacy Act of 1986	Private parties	Extends Title III protections and requirements to new forms of voice, data, and video communications such as cellular phones, electronic mail, computer transmissions, and voice and display pagers.
Driver's Privacy Protection Act (1994)	Private parties	Enables motorists to "opt-out" of allowing the state to sell or give their personal identifiable information; recently upheld by the Supreme Court as a "thing of interstate commerce" that can be regulated by Congress.
Electronic Freedom of Information Act (1996)	Federal Government	Updated the Freedom of Information Act of 1966 (FOIA), which allowed any person the right to obtain federal agency records unless the records (or part of the records) are protected from disclosure by any of the nine exemptions contained in the law. Extends the FOIA to make available material on the Internet.
Health Insurance Portability and Accountability Act (HIPAA-1996)	Private parties	Requires healthcare facilities to implement security policies and systems to protect patient confidentiality. HIPAA only covers the security of the information and does not address information sharing.
Children's Online Privacy Protection Act (1999)	Private parties	Prevents personal information from being collected online from children younger than 13 years old without parents' consent via email, mail, fax, telephone, and/or credit card.*
Financial Services Modernization Act (2000) (Gramm-Leach-Bliley Act)	Private parties	Requires banks to offer "opt-out" of the disclosure of individual's personal information to unaffiliated entities; allows the sharing of medical information between banks and insurance companies without individual's knowledge and consent.
Safe Harbor Principles (March 2000)	Private parties	Tentative agreement between the U.S. and the E.U. that the U.S. self-regulatory system abides by the rules of the E.U.'s Privacy Directive. E.U. citizens are allowed access to their personal data for review and correction. U.S. companies cannot sell personal data without the permission of the E.U. citizen; Perceived to give Europeans more privacy protection than Americans enjoy, yet less than Europeans enjoy in their home countries.

* On June 22, 2000, the US Court of Appeals for the Third Circuit in Philadelphia upheld a lower court ruling barring enforcement of the Child Online Privacy Protection Act (COPPA). The unanimous ruling found that Inter-content regulation laws violate the First Amendment.

The following table is a sample of pending privacy legislation in the 106th Congress. Some of the bills pending are somewhat limited in scope. For instance, one establishes a commission to study the privacy issue. Other bills are broader, such as S.864, which gives consumers the right to opt-out of allowing entities to share or sell their information.

Selected Pending Legislation in 106th Congress

Bill Number	Name of Bill and Sponsor	Summary
HR 4049	Privacy Commission Act (Hutchinson/Moran)	Establishes the Commission for the Comprehensive Study of Privacy Protection.
H.R.3560	Online Privacy Protection Act of 2000 (Frelinghuysen)	To require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet. To provide greater individual control over the collection and use of that information, and for other purposes.
H.R.1685	Internet Growth and Development Act of 1999 (Boucher)	Provides for the recognition of electronic signatures for the conduct of interstate and foreign commerce; restricts the transmission of certain electronic mail advertisements; authorizes the Federal Trade Commission to prescribe rules to protect the privacy of users of commercial Internet Web sites; promotes the rapid deployment of broadband Internet services, and for other purposes.
S. 854	E-Rights (Leahy)	Gives consumers the right to "opt-out" and establishes standards for law enforcement to access encrypted communications and files.
S. 809	Online Privacy Protection Act (Burns/Wyden)	Requires privacy disclosures on Web sites, "opt-out" option and allows consumers to access their own data.
S. 1901	Privacy Protection Study Commission (Kohl)	Establishes Privacy Commission to evaluate the Freedom of Information Act (FOIA) and E-FOIA.
S. 2063	Secure Online Communications Act of 2000 (Torricelli)	Amends the Electronic Communications Privacy Act of 1986; restricts disclosure of personal info without request of consumer.
H.R. 2457	Genetic Nondiscrimination in Health Insurance and Employment Act (Slaughter)	Prohibits insurers from restricting enrollment or adjusting fees on the basis of genetic information; prohibits genetic discrimination in all areas of employment; forbids insurers and employers from requiring genetic testing.
H.R. 4246	Cyber Security Information Act (Davis)	Grants exemptions from FOIA when private companies share information about computer vulnerabilities with the federal government.[15]
Clinton Administration Privacy Initiative		President's legislative package would enable consumers to demand the financial service company not divulge their personal information to any other firm, including affiliates; provides stricter safeguards for medical records and data detailing personal spending habits.

International

According to a report by Privacy International and the Electronic Privacy Information Center, nearly every country in the world recognizes a right of privacy explicitly in its Constitution. In some very recently written constitutions, namely that of South Africa and Hungary, specific rights to access and control of one's personal information are included.[16]

Countries around the world are moving towards comprehensive privacy and data protection laws. Most of the new laws are based on the models introduced by the Organization for Economic Cooperation and Development, and the Council of Europe.
There are three main reasons for the movement towards privacy legislation:

- To remedy past privacy violations that occurred under previous authoritarian regimes;
- To promote electronic commerce; and
- To ensure laws are consistent with the European Union's (E.U.) Data Protection Directive. Many of the East European countries hope to join the E.U. in the future. In addition, many countries want to conduct business with the E.U. and need to be compliant with their privacy policies.[17]

Several countries around the world have made strides in protecting personal privacy. In this small sampling of countries, China has the least privacy protection, Australia is experimenting with a hybrid of self-regulation and government regulation, while the European Union has the strictest privacy directives.

Australia
In 1998, Australia passed the National Principles for the Fair Handling of Personal Information. This Act provides protection for the following:

- Personal information held by governmental agencies;
- Personal tax file numbers used by individuals and organizations; and
- Information about a person's credit held by credit reporting agencies and credit providers.[18]

The Act mainly applies to government agencies, but the private sector is subject to the Act in that credit agencies and providers must comply with the credit reporting rules and all entities who hold and use tax file number information must comply with the tax file number guidelines.

After the passage of the privacy act, the Australian government announced that it would combine self-regulation with governmental control. The government will not intervene in those industries that have adopted strict privacy policies. However, the government will dictate privacy policies to those industries that have not adopted strict privacy policies. In April 2000, the Attorney General of Australia introduced a Privacy Amendment Bill pertaining to more outlined privacy procedures for the private sector to follow. The bill has not yet passed. Australia also has a privacy commission; details are included in Appendix III.

Canada
Canada passed a Privacy Act in 1983 to address privacy concerns that developed with the prevalent use of the personal computer. This law outlined privacy protections for information held by the public sector. The 1983 Privacy Act gave individuals the right to examine information held by 110 federal government departments and request that errors be corrected. If the request is refused, the individual can require that a statement of disagreement be attached to the information. In addition, the law requires the Canadian federal government to:

- Limit its collection of personal information;
- Collect information directly from the person concerned, whenever possible;
- Inform the person on how the information will be used;
- Not use the information for other purposes, unless allowed by law; and
- Not disclose personal information unless specifically allowed by law.[19]

On April 13, 2000, the Canadian Parliament passed the Personal Informational Protection and Electronic Documents Act. This new privacy act protects personal information that is collected, used, or disclosed in the course of commercial activity."[20] The Act specifies requirements for e-commerce and other marketers to obtain the explicit consent of consumers before providing their personal information to third parties. Since the 1983 Privacy Act only applied to the public sector, the Canadian Parliament felt that equal protection needed to be provided in the private sector. The goal was "so that all Canadians, no matter where they live, will be assured of privacy protection." The legislation, which goes into effect on January 1, 2001, can be accessed at: http://www.privcom.gc.ca/english/02_06_e.htm

The Canadian federal government and almost every Canadian province have privacy commissions. One of the best known of the commissions is that of Ontario's. Appendix III includes detailed information of the responsibilities of both the Canadian federal and the Ontario privacy commission.

Ontario, Canada

Ontario, Canada provides two statutes that protect personal privacy in the public sector. The Freedom of Information and Protection of Privacy Act 2000 applies to Ontario's provincial ministries and agencies, boards, commissions, community colleges and district health councils. The Municipal Freedom of Information and Protection of Privacy Act 1998 applies to municipalities, local boards, agencies, and commissions. Both acts protect the privacy of personal information in government records, gives citizens the right to request access to records containing their own personal information, and gives citizens the right to *request* correction of that information. In addition, both acts include rules regarding the collection, retention, use, disclosure, and disposal of personal information in government custody.[21]

China and Hong Kong

While China does not have a history of protecting their citizens' privacy rights, it does grant limited privacy rights within the constitution and within regulations dealing with Internet security and management. [22]

Hong Kong protects citizen privacy more extensively. The Personal Data (Privacy) Ordinance protects any data relating directly or indirectly to a living individual (data subject). Its provisions apply to any person (data user) that collects, maintains, or processes personal data. It is assumed that this means both private and public sector entities are subject to this law. The law states that data users must follow the fair information practices as outlined in the Ordinance. http://www.pco.org.hk/ord/section_00.html
The Ordinance also gives data subjects the right to confirm where their personal data is held, to obtain a copy of the data, and to have the data corrected.[23]

European Union

While the European Union trails behind the United States in personal computer use and Internet penetration, its privacy laws are the most comprehensive in the world. The E.U. has strict laws and policies on how personal information can be used, both online and offline. In 1995, the European Union released Directive 95/46/EC or otherwise known as the E.U. Privacy Directive. The Directive's main provisions are outlined below:

1. It requires E.U. member states to create and enforce national privacy policies with the recognition that personal data is able to flow freely from one member state to another, while also safeguarding the rights of individuals.
2. It prevents unauthorized transmission of personal information to countries that do not ensure adequate protection. This essentially makes the Directive a global standard. Nations wanting to conduct trade with the E.U. are forced to create strong personal information privacy policies in order to conduct and maintain trade and business partnerships.
3. It mandates sanctions against those entities that violate the strict privacy policies of the Directive. Each member state enforces the national privacy laws of the country. The sanctions have ranged from a fine of a few thousand dollars to the ruining of one's business

reputation. Loss of one's business reputation can be more damaging than paying a fine in a society that values personal privacy.

4. It requires the creation of a privacy commission in each member country to address consumer complaints on a full time basis. The commissions should also educate the public on personal information privacy issues. It is expected that countries that do business with Europe have similar oversight.
5. It gives citizens and consumers the following rights concerning their data:

    - right to know where the data originated,
    - right to have inaccurate data corrected,
    - right of recourse in the event of unlawful processing,
    - right to withhold permission to use data, and
    - right to opt-out free of charge from direct marketing schemes.[24]

The Directive has major implications for U.S. trade and electronic commerce. Before the electronic era, the difference in personal privacy policies between the U.S. and Europe was minimal. In the current world of international trade, the privacy issue has the potential to block U.S. companies from conducting business or expanding overseas. Similarly, online shoppers, both domestic and international, may choose not to buy from U.S. companies because of privacy concerns.

Russia
In Russia, personal privacy is protected by the Law of Russian Federal on Information, Informatization, and Information Protection, which was passed in 1995. The law applies to both the public and private sectors and defines individual privacy rights, the lawful use of information, and the lawful use of information technologies. The law is currently being updated to comply with the E.U. privacy directive.[25]

New Zealand
The Privacy Act of 1993 applies across both public and private sectors and directly concerns the informational privacy of individuals. The Act includes twelve information privacy principles that serve as the basis of the collection, use, retention, and access of personal information
www.privacy.org.nz/people/fact3-0.html

All of the selected countries previously discussed have adopted a regulatory model of privacy protection. In the regulatory model, a public official enforces a comprehensive data protection law. This office is known as a Commissioner, Ombudsman, or Registrar. The official monitors compliance with the law and is responsible for public education on privacy.

Privacy Commission

Many countries have adopted the regulatory model of privacy protection and have established a privacy commission and Commissioner. Just as privacy policies differ from entity to entity, so do the scope and authority of all commissions. Some commissions are merely fact-finding, report to a legislative or an executive body, while others have rule-making and regulatory authority.

The following questions were explored concerning privacy commissions:

1. What responsibilities does the commission have?
    - Regulatory?
    - Fact-finding?
    - Educational?
    - Policy Making?
2. Is the commission independent to other governmental bodies and private industries?
3. What sectors does the commission protect? Public and/or private?
4. What is the composition of the various commissions?

Major Findings

The five countries examined here all have a privacy law that the commission/commissioner enforces. New Zealand is the only nation that had a Privacy Commission before a privacy law was passed. As the following table demonstrates, four out of five are independent government bodies. The research did not reveal how the privacy commissions were composed or how the privacy commissioners were chosen. Most privacy commissions investigate complaints, educate the public, provide information and advice to government agencies, and provide policy analysis of pending legislation and current trends. Ontario, Canada is the only jurisdiction examined whose law only applied to the public sector. Thus, the privacy commission for Ontario monitors only government agencies. Appendix III, Privacy Commissions, provides more detail of the responsibilities and unique practices executed in each jurisdiction. The Unique Practices section under each jurisdiction is of particular interest as Texas examines the potential of a privacy commission for the State.

Country	**Responsibilities**						**Scope of Coverage**
	Year Commission Established	Independent	Investigate Complaints and audit	Education	Information and Advice	Policy	Public or Private Sector
Australia	1988	X	X	X	X	X	Both
Canada	1983		X	X	X	X	Both
Ontario, Can	1988	X	X	X	X	X	Public
Hong Kong	1996	X	X	X	X		Both
New Zealand	1991	X	X	X	X	X	Both

Recommendations

The State of Texas must act now to protect citizen privacy. Privacy is not an issue that can be overlooked in government's effort to serve the public through online means. Once personally identifiable data is released, there is no way to determine who has access to the data and the purposes the data is used. Recent studies and surveys suggest that the public is concerned about who has personal information about them and what that information is being used for. A guide to protecting individuals' privacy is the Code of Fair Information Practices, which can be found in Appendix II. By implementing these recommendations, Texas State government will be taking the first steps in ensuring privacy of personal information given through the State portal, raising the public's comfort level, and increasing the use of government services online.

Each of the possible solutions is prefaced by a code that directs the reader to the specific government body the recommendation most concerns:

- *LEG* – These are recommendations that require legislative action in order to be implemented.
- *STATE* – These are recommendations that can be implemented by state agency action.
- *TF* – Task Force initiatives may require setting portal policies and standards.

1. (LEG/STATE) State agencies should be very deliberate about every piece of data collected on individuals, and collect only that data for which there is a legitimate governmental need as determined by the agency's board.

2. (LEG) Citizens should have the right to review and challenge the accuracy of the information collected and held about them through the State portal. ..

3. (STATE) Citizens should be provided clear and complete information about the privacy policies under which state agencies operate. Privacy policies should avoid "legalese" and should describe why and how personal information is collected and how it is used.

4. (STATE) Agencies must be held accountable for faithfully executing their privacy policies and the law. This includes having strong security measures in place to safeguard private information against unauthorized intrusions and coordinate efforts with authorized third parties to perform unannounced annual checks of portal participating governmental agencies to ensure that privacy policies are being adhered to.

5. (LEG) The Legislature should establish a privacy commission that is authorized to do the following:

    - Investigate complaints and assist government agencies routinely in complying with applicable privacy rules and statutes;
    - Educate the public on how to protect their privacy and how to access public information from state government;
    - Provide a Privacy Hotline where individuals and government agencies can get general information and advice concerning their privacy rights under Texas law;
    - Conduct policy analysis on proposed and existing legislation in concert with the Office of the Attorney General for privacy implications and conduct research into technological and social developments that can affect personal privacy;
    - Meet with records management and online privacy personnel in each agency annually to identify and address privacy concerns of agencies and to determine compliance with the Public Information Act and potential privacy act(s).

Appendix I: Understanding Privacy

Privacy protection is understood as the right of individuals to control the collection, use, and dissemination of their personal information that is held by others.[26] Personal information or personally identifiable information includes but is not limited to name, address, e-mail address, telephone number, credit card number, social security number, occupation, income, family information, interests, and education. In 1973, the United States, Canada, and Europe developed the Fair Information Practice Principles based on the fundamental right to privacy. The four Fair Information Practice Principles are currently being used as benchmarks by government agencies around the world. The Practices are as follows:

1. Notice/Transparency
   This principle requires that government and business organizations provide consumers clear and conspicuous notice of their information practices, including what they collect, how they collect it, how they use it, whether they disclose the information collected to other entities, and whether other entities are collecting information through as well.

2. Choice/Fairness
   Consumers should be given a choice as to how their personal identifying information is used beyond its original intent. Permission to use the information for other purposes extends to internally marketing back to the customer and disclosing the data to other entities.

3. Access
   If the access principles are instituted, consumers would be given reasonable access to the information an entity has collected about them, including an opportunity to review information and to correct inaccuracies or delete information.

4. Security
   All entities, business and government, would be required to take reasonable steps to protect the security of the data they collect from their customers.[27]

Many privacy advocates claim that industry and government must recognize that individuals should not be required to negotiate or choose among the Fair Information Practices. Privacy only exists when all the Fair Information Practices are enforced.

As of yet, many governmental entities in the United States have not accepted the Practices for wide spread use. The evolving technology has created a dramatic increase in the collection, use, and movement of information and has eroded the perception of personal privacy in the United States. The rise in access to information has removed the control of personal information from those whom it pertains and has given it to businesses that exist solely to profit from the sale of such personal information. Many are blaming the Internet for the growth of information proliferation, but privacy erosion started in the off-line world.

Privacy in the Off-Line World

For many years, businesses have been collecting personal information of consumers. Information is collected every time a consumer orders from a mail order company, sends in a sweepstakes form, subscribes to a magazine, uses a credit card, and joins a “discount buyers club.” After such information is collected it can be used for advertising, sold or exchanged with other companies, or run through a process called data matching. Data matching is a process where multiple databases are merged together using a common identifier like a social security number. This allows the company or direct marketer to learn more about the consumer’s hobbies, habits, interests and lifestyle, and market their product accordingly. The marketer then sends customized advertisements and coupons to the consumer according to their data.

Privacy in the Online World

"Self-regulation alone is unlikely to provide online consumers with the level of protection they seek and deserve."
-- Federal Trade Commission Chairman Robert Pitofsky

Business Information Privacy Practices

Marketing schemes do not exist in the offline world alone. Click streams, Web bugs, and cookies are being used in a variety of Web sites to learn more about the user. Click streams are new tracking technologies that allow the server or Web site to track a very long and detailed path of where that individual was and exactly what sites, buttons and links he or she clicked on. Web bugs are codes that can identify a particular computer and help advertising services far removed from the site determine whether electronic promotions are well-read and effective in prompting someone to buy a product. They often work with cookies to greatly enhance the ability of outside observers to track and analyze activity, most often without a computer user's knowledge. Cookies are small data packages that sites put on a user PC to store information such as a password and to gather information about users by tracking their movements through the site. Combined, this anonymous information can create a remarkably detailed dossier of one's life when connected to a computer Internet Protocol address, name, and address.

Currently, there are no federal regulations concerning Internet privacy for anyone over thirteen years old. The Internet industry has been self-regulated since its inception. Internet privacy has increasingly become a growing concern for consumers because of media attention of privacy invasions.

The business community is divided between protecting consumer privacy and using consumer data to make profits. Businesses can use the personal information of its customers to improve marketing strategies and to sell the information to other firms and individuals. According to the Harvard Business Review, the average price of acquiring a new e-customer is $100. Many e-tailer's average customer acquisition cost is higher than the average profit that that customer will bring to the company in the long run.[28] Although the entry cost into e-business is high, the cost of selling customer information is extremely profitable. In 1995, the Internet industry as a whole was estimated to have made over $3 billion annually from the selling of personal information.[29] Assuredly, this figure has grown exponentially in the past six years.

The selling of consumer personal information is a double-edged sword. Although companies that sell information profit monetarily, others in the industry stand to lose billions of dollars as a direct result of consumers fearing their privacy will not be honored and their data will be sold. In 1999, Jupiter Communications Inc. estimated that e-commerce revenues will drop $18 billion and advertising revenues will drop $2.7 billion due to consumer distrust.[30] Because of the potential high loss of revenue, the Internet community is attempting to balance the desire to attain data for marketing purposes and the need to appease the public wariness of the Internet.

Several coalitions have formed in an effort to better self-regulate the industry. NetCoalition, which includes Amazon.com Inc, eBay Inc, America Online Inc., and Lycos Inc., sent a letter in May 2000 urging their e-business colleagues to protect consumer privacy more seriously.[31] The letter urges companies to adopt strict, clear, and comprehensive privacy policies. The Personalization Consortium has approached the problem differently. The consortium, which includes American Airlines, BroadVision, Double Click, Elity Systems, Epiphany, Frequency Marketing, KPMG Consulting and Pricewaterhouse Coopers, has developed guidelines concerning the type of data that can be collected on their users. Members of the consortium are required to let users know what data is being collected, allow users to opt-out of the collection, and conduct a yearly privacy audit of sites.[32]

Technological Solutions for the Consumer

The threat of having "Big Brother" watching over us or being a victim of identity theft has sparked debate over whether the federal government should regulate Internet privacy. The FTC Advisory Committee on Online Access and Security submitted a report in May 2000 concluding that self-regulation in the Internet industry is an insufficient means to protect individuals' privacy. The report suggests that new legislation

set a standard level of privacy for consumers. Until the government acts, many consumers are looking to new technologies for a solution to their privacy concerns.

In June 2000, President Bill Clinton publicly supported a new technology to help protect consumer privacy on the Internet. Clinton even went so far to propose it as the standard on the White House and Commerce Department Web sites. Developed by the World Wide Web Consortium, P3P, Privacy Preference Project, allows users to set their own levels of privacy when browsing the Internet. This technology relieves the user from having to read and interpret the privacy statements of each Web site. The browser will only allow the user to visit sites that follow their selected preferences.

Businesses have also stepped up to the challenge of providing online privacy. A company called Privada (www.privada.net) provides a system where users can make all of their Internet transactions completely anonymously, including email, Web browsing, online chats, and e-commerce.. Another product called *Freedom* by Zero Knowledge Systems (www.freedom.net) uses sophisticated encryption software to cloak the true identity of an Internet user behind a pseudonym that the user, company, or others do not know. For an annual fee of $49.95, the user can register up to five different identities that identify the user while visiting Web sites, sending e-mail, and participating in other Internet activities. The software prevents anyone from intercepting data packets during the transmission.[33]

Privacy and Economic Access: Are there variations in privacy?

Some privacy experts contend that a privacy divide, much like the digital divide is developing. The contention is that the privacy discussion only addresses the privacy of middle and upper income households. Lower income households have no privacy "choice" when receiving benefits from the government or when they attain free services from a company. While the privacy divide is not directly related to e-government and the development of the Texas State portal, but its implications will effect privacy legislation in the future. For this reason, a discussion on the topic is necessary. Computer companies, Internet start-ups and others naturally want to increase their customer base. Recently, these companies have started offering free hardware, software, and services. These free services help low-income families keep up with computer and Internet technologies, but they do not come without a price. In order to obtain free or discounted PCs and Internet access, people are required to allow companies to track their surfing habits, which may eventually lead to the linking one's Web surfing habits to one's offline identity.[34] Granted that some individuals may not mind giving up a little privacy for service, but they should be aware that their personal information can be widely used and distributed. Privacy should be a right that everyone in the U.S. has, regardless of income.

Appendix II: Privacy Policies and the Code of Fair Information Practices

Privacy policies vary widely from country to country. The growing division between businesses and citizens in the U.S. does not exist in all countries. In the U.S., many businesses view personal privacy regulation as an impediment to new channels of revenue. In contrast, business groups in Canada, New Zealand, and Europe have been lobbying for privacy legislation in the hope that rules defining how companies use personal information will give consumers more confidence in using electronic commerce.

Unlike Europe and other nations, the United States has accepted a self-regulatory model concerning data protection. In 1998, the Federal Trade Commission published a set of guidelines by which self-regulation could continue. Among these guidelines is the requirement that Web sites post information on their policies for collecting and using information, otherwise known as Privacy Policies. After two years of self-regulation, the FTC conducted a survey, which reviewed the nature and substance of U.S. commercial Web sites and recommended legislation in order to ensure that the personal privacy is protected.

Whether or not Congress passes Internet privacy legislation in the future, it is essential that all Texas State sites, especially Texas Online, develop strong and enforceable privacy policies that respond to citizen concern. It is important to note that while the Department of Information Resources develops standards for state privacy policies, DIR does not write the privacy policy of each individual state agency or governmental entity. If strong and easily understood privacy policies are not developed by all Texas State sites,, privacy will become a major issue that severely impedes progress in Texas Online and e-government in general. The most widely adopted benchmarks used for privacy policies are the Code of Fair Information Practices:

1. Notice/Transparency
   Consumers should be provided with a clear and conspicuous notice of the governmental body's information practices, including what they collect, how they collect it, how they use it, whether they disclose the information collected to other entities, and whether other entities are collecting information through them.

2. Choice/Fairness
   Consumers should be given a choice as to how their personal identifying information is used beyond its original intent. One of the best and most popular methods of protecting privacy online is to combine elements of opt-in and opt-out. In an opt-out situation, the site is free to gather and sell information unless the subject specifically tells them not to. Opt-in situations forbids the gathering and selling of information without the specific permission of the subject. Permission to use the information for other purposes extends to internally marketing back to the customer and disclosing the data to other entities. Many surveys and reports stated that consumers and citizens prefer the opt-in approach. In order to acquire and retain citizen trust in Texas Online and e-government, it is essential to institute the opt-in approach.

3. Access
   Consumers should be given reasonable access to the information the governmental bodies have collected about them, including an opportunity to review information and to correct inaccuracies or delete information.

4. Security
   All entities, business and government, would be required to take reasonable steps to protect the security of the data they collect from their customers.[35]

In addition to the Code of Fair Information Practices, it is imperative that each agency's privacy policy on Texas Online be consistent with the Public Information Act. Until there is a change in the Public Information Act, it would be helpful to note on all Texas Online privacy policies that the policy for one

Web page may be different from that of another Web page on the site. Users must understand that the privacy protections and data management policies at the Department of Insurance may be different than those at the Comptroller of Public Accounts.
The state's Department of Information Resources has ruled that as of July 1, 2000 (http://www.state.tx.us/Standards/S201-12.htm) the home page of all Texas state Web sites, and any new or changed key public entry points must have a privacy policy which addresses the following:

- Use of server logs and/or cookies;
- Information collected by other technologies and processes;
- Information collected via e-mail and Web-based forms. A Web-based form must post a link to the policy. The form may include a provision for the individual to opt-out of sharing the information with another party, or a warning that the information may be a public record and therefore subject to the Texas Public Information Act;
- Web pages designed for children must comply with all applicable federal and state laws intended to protect minors;
- State agencies must plan on implementing P3P* on the home page and key public entry points to a state agency Web site; and
- Prior to providing access to information or services on a state Web site that require user identification, each state agency must conduct a transaction risk assessment, and implement appropriate security and privacy safeguards. At a minimum, state Web sites that require a citizen to enter the following information shall use an SSL session or equivalent technology to encrypt the data:

  - Both the individual's name and other personal information, such as a SSN;
  - Transaction payment information; or
  - An individual's identification code and password.

The National Electronic Commerce Coordinating Council (NECCC) produced "Privacy Policies: Why You Need One, A Framework for states and Localities" in June 2000. This paper provides an analysis of best practices and privacy policy models, state privacy policies, and Internet security.

* The Platform for Privacy Preferences Project (P3P) is a standard developed by the World Wide Web Consortium, that enables Web sites to express their privacy practices in a format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. The World Wide Web Consortium will host an interoperability demonstration of P3P products on June 21, 2000.

Appendix III: Responsibilities and Practices of Privacy Commissions

This appendix offers a detailed look at the composition, responsibilities, and unique practices of the various privacy commissions around the world.

Australia

The Australian Office of Federal Privacy Commissioner is an independent office created by the Privacy Act of 1998.

Commissioner Responsibilities

The Australian Office of the Federal Privacy Commissioner holds the following responsibilities:

1. *Information and Advice*
   The Office operates a Privacy Hotline where individuals and government organizations can get general information and advice concerning their rights under the Privacy Act and related legislation, privacy issues and best practices in privacy standards, and how governmental agencies can comply with privacy legislation.
2. *Policy*
   A section of the office provides policy advice to ministers, government entities and private companies. They also examine proposed legislation for privacy implications and conduct research into technological and social developments that can affect personal privacy.
3. *Complaint handling and audits*
   The Office investigates complaints from private individuals concerning violations of the Privacy Act. They also conduct routine audits of government entities that handle personal information.
4. *Education*
   The Office publishes information and fact sheets about privacy issues for the public. In addition, they maintain an information Web site.

Unique Practices

Within the realm of the public sector, Australia has instituted three unique concepts not found in any of the examined countries' commissions:

- *Privacy Contact Officers (PCOs)*
  These officers are the first points of contact concerning privacy issues in each governmental body. Privacy complaints are first directed to an agency's PCO before the Office of the Federal Privacy Commissioner. The Privacy Commissioner's Office organizes a conference with all the PCOs two to three times a year to discuss current privacy issues.
- *Public Interest Determinations*
  The Privacy Commissioner has the power to determine that an act or practice of an agency constitutes a violation of one of the Information Privacy Principles (http://www.privacy.gov.au/private/index.html) in which the Privacy Act is based. If such a determination is made the act or practice must cease. To date, seven such determinations have been applied for and six have been issued.

Canada

The Privacy Commissioner of Canada is a specialist ombudsman, appointed and accountable to the Parliament that monitors the federal government's collection, use, and disclosure of personal information.

Commissioner Responsibilities
The Privacy Act of 1983 mandates the Commissioner to:

- investigate complaints,
- monitor compliance with the Privacy Act,
- study and report on emerging privacy issues, and
- act as a privacy resource center for individuals and organizations.[36]

Unique Practices
Canada does not have any practices that were found unique among the small sample examined. Although, Ontario, Canada has practices not found in other jurisdictions.

Ontario, Canada

Created in 1988, the Ontario Privacy Commission is considered the model of privacy commissions by privacy advocates.

Commissioner Responsibilities
Under the Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act, the Information and Privacy Commissioner of Ontario (IPC) is responsible for the following:

- "resolving appeals from refusals to provide access to information;
- investigating privacy complaints about information held by government organizations;
- ensuring that government organizations comply with the access and privacy provision of the Acts;
- educating the public about Ontario's access and privacy laws; and
- conducting research on access and privacy issues, and providing advice and comment on proposed government legislation and programs."[37]

Unique Practices

- *Protection of personal information*
  In Ontario, government agencies must refuse disclosure of Cabinet records, third party information if supplied in confidence, and personal information about individuals other than the requester. The last mandatory exemption makes sweeping protection of individual privacy a reality.
- *Statement of Disagreement*
  Individuals are given the right to access of their personal information. They can also request correction of such information if they believe that there is an error or omission. The government body does not always accept these requests. When a request is refused, the individual can require the governmental body to attach a statement of disagreement to be attached to the information in question. In addition, the individual can also require that all parties to whom the information has been disclosed within the last year be notified of the correction or statement of disagreement.[38]

Hong Kong, China (since July 1, 1997)

Most of the nations that have a privacy commission are in Europe or have European ties. Hong Kong is no exception. The Privacy Commissioner's Office is result of British influence during its over 150 years of control of this entity. The Privacy Commissioner's Office (PCO) is an independent statutory body set up to oversee the enforcement of the Personal Data (Privacy) Ordinance, which was passed in 1996.

Commissioner Responsibilities
The Privacy Commissioner plays an educational, regulatory, and enforcement privacy role in Hong Kong. The Commissioner promotes awareness of the Ordinance and gives practical advice on compliance

procedures. He or she also investigates suspected violations and enforces the law. Non-compliance can carry a maximum penalty of $25,001 to $50,000 and two years imprisonment.[39]

Unique Practices
In addition to these tasks, the Hong Kong Privacy Commissioner also conducts the following:

- *Data Matching Approval*
  The Commissioner approves requests from data users to conduct data matching of personal data; and
- *Maintains a Registry of Data Users*
  The Commission has the power to specify what classes of data users are required to submit annual reports. This is used to compile a register of data users for public inspection.[40]

New Zealand

New Zealand established a Privacy Commissioner in 1991, two years before instituting a privacy act.

Commissioner Responsibilities
In addition to the standard responsibilities of a privacy commissioner, (investigating complaints, educating public, and making public statements) the New Zealand Commissioner is also authorized to conduct the following:

- Grant exemptions to the Privacy Act in the cases that public interest outweighs the interference with privacy;
- Issue codes of practice which may modify the application of any of the information privacy principles, modify the application of any of the public register privacy principles, or exempt any action from the principles;
- Monitor and report on authorized information matching programs. The Privacy Act places restrictions on statutory information matching programs implemented by the public sector. The Act requires that notice be given to the individual before information matching is done.

Unique Practices
The fore-mentioned Commissioner responsibilities make New Zealand unique among this sampling of nations with privacy commissions. In addition to these, the New Zealand Privacy Act contains four *public register privacy principles,* which limit:

- "the manner in which information can be made available from public registers;
- resorting or combining public register information for commercial gain;
- electronic transmission of public registers;
- charging for access to public register information."[41]

In addition, New Zealand also has a *Privacy Officer* within each agency. They are similar to Australia's Privacy Contact Officers in that they encourage compliance within their agency and deal with the public concerning requests for personal information. However, the New Zealand Privacy Commissioner does not hold conferences with all the agency Privacy Officers, but instead works one-on-one with an agency privacy officer when there is a complaint made against the agency.

United States

The United States does not currently have a privacy commission. The Hutchinson Privacy Commission Act is the only bill moving toward passage out of all the privacy bills up for debate in Congress this year. The Privacy Commission Act (HR 4049) establishes the Commission for the Comprehensive Study of Privacy Protection to study and report to Congress and the President on issues relating to protection of individual privacy and the appropriate balance to be achieved between protecting such privacy and allowing appropriate uses of information. The Commission would have a year to study the privacy issue before presenting final recommendations to Congress.

Conclusions and Recommendations

Responsibilities

Privacy commissions around the world are experimenting with a variety of different methods to protect the personal information of their citizens both in the private and the public sectors. The potential Texas Privacy Commission should adopt five common responsibilities of the privacy commissions examined:

- Analyze complaints and assist government agencies in complying with applicable privacy rules and statutes;
- Educate the public on how to protect their privacy and how to access public information from state government;
- Provide a Privacy Hotline where individuals and government agencies can get general information and advice concerning their rights under the potential privacy act;
- Conduct policy analysis on proposed and existing legislation in concert with the Office of the Attorney General for privacy implications and conduct research into technological and social developments that can affect personal privacy;
- Meet with agency "privacy officers" annually to identify and address privacy concerns of agencies and to determine compliance with the Public Information Act and the potential privacy act(s).

In addition, the three Unique Practices highlighted below should be taken into consideration as possible responsibilities and practices for a Texas Privacy Commission:

- *Privacy Contact Officers (PCOs)*
  These officers are the first points of contact concerning privacy issues in each governmental body. Privacy complaints are first directed to an agency's PCO before the Office of the Federal Privacy Commissioner. The Privacy Commissioner's Office organizes a conference with all the PCO two to three times a year to discuss current privacy issues.
- *Personal Information Digest*
  All federal government agencies are required to maintain a record of the various types of personal information kept, the purpose for which the records are kept, the population that the records are kept on, and the period of time the records are kept. The Privacy Commissioner collects this information and organizes it into a Personal Information Digest. This digest is accessible to most Commonwealth employees. Private individuals can attain extracts or full copies of the digest for a fee.
- *Protection of personal information*
  In Ontario, government agencies must refuse disclosure of personal information about individuals other than the requester. This mandatory exemption makes sweeping protection of individual privacy a reality

Appendix IV: Additional Resources

This appendix provides additional resources concerning privacy both online and off-line. Many of those listed below are not found in the endnotes of the privacy paper.

Privacy Organizations Online

American Civil Liberties Union – The ACLU conducts extensive litigation on Constitutional issues, including privacy.
http://www.aclu.org

Center for Democracy and Technology - CDT seeks practical solutions to enhance free expression and privacy in global communications technologies.
http://www.cdt.org/

Computer Professionals for Social Responsibility - CPSR is a public-interest alliance of computer scientists and others concerned about the impact of computer technology on society. They work to influence decisions regarding the development and use of computers because those decisions have far-reaching consequences.
http://www.cpsr.org

Electronic Privacy Information Center – EPIC focuses public attention on emerging privacy issues in all sectors through litigation, conferences, and reports.
http://www.epic.org

Electronic Frontier Foundation – EFF is a non profit, non-partisan organization that works to protect civil liberties, including privacy and freedom of expression concerning computers and the Internet.
http://www.eff.org/

Federal Trade Commission - The Federal Trade Commission enforces a variety of federal antitrust and consumer protection laws. The Commission also advances the policies underlying Congressional mandates through cost-effective non-enforcement activities, such as consumer education.
http://www.ftc.gov/

Online Privacy Alliance – The alliance includes a diverse group of corporations and associations that are working to introduce and promote business-wide actions that create an environment of trust and foster the protection of individuals' privacy online.
http://www.privacyalliance.org

Privacy Council – The Privacy Council assists businesses implement smart privacy and data practices. They also bring in leading privacy advocates who are experts in the development of training and educational programs that fit a company's needs.
http://www.privacycouncil.com/index.htm

Privacy.net – Privacy.net is a consumer organization dedicated to educating consumers on privacy issues including, how they are tracked on the net, current events, and third party activities.
http://privacy.net

Privacy International - Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns throughout the world on issues ranging from wiretapping and national security activities, to ID cards, video surveillance, data matching, police information systems, and medical privacy.
http://www.privacyinternational.org/

PrivacyRatings.org – This site rates the privacy polices of over 30,000 Web sites using strict and objective criteria.
http://privacyratings.org/

Privacy Rights Clearinghouse – The PRC offers consumers a unique opportunity to learn how to protect their personal privacy. They offer publications that provide in-depth information on a variety of informational privacy issues, as well as practical tips on safeguarding personal privacy.
http://www.privacyrights.org

Certification Programs

These third-party programs provide "seals of approval" or "trustmarks" to inform consumers that the site has met the minimum privacy and security standards.

BBBOnline - Better Business Bureau Online	http://www.bbbonline.org
CPA Webtrust	http://www.cpawebtrust.org/
PrivacyBot	http://www.privacybot.com
TRUSTe	http://www.truste.org

Papers and Articles

Banisar, David and Simon Davies. "Privacy and Human Rights: an International Survey of Privacy Laws and Practice." Privacy International and the Electronic Privacy Information Center.
Http://www.gilc.org/privacy/survey/intro.html.

Federal Trade Commission. "Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress." May 2000.

National Electronic Commerce Coordinating Council (NEC3) Privacy 2000 Workgroup. "Privacy Policies: Do You Have One? A Guide for State and Localities." June 2000.

Senate Majority Task Force on the Invasion of Privacy. Senate Majority Leader Joseph L. Bruno. March 2000.

EMA Privacy Policy Tool Kit: Access to , Use, and Disclosure of Electronic Messaging on Company Computer Systems in the 21st Century.

Cate, Fred H. and Richard J. Varn. "The Public Record: Information Privacy and Access—A New Framework for Finding the Balance" (1999).

Legislation

European Union. Directive 95/46/EC of the European Parliament and of the Council. 24 October 1995. Provides protection of individuals with regard to the processing of personal data and on the free movement of such data
http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

Texas. Office of the Attorney General. "Privacy Acts of the States and the United States."
http://www.oag.state.tx.us/notice/privacy_table.htm.

Texas. Office of the Attorney General. "Information held by Governmental Bodies deemed Private or Confidential by Texas Constitution and Statutes."
http://www.oag.state.tx.us/notice/privacy_statutes.htm

Securities Industry Association. "State Privacy Legislation 2000 Session."
http://www.sia.com/government_relations/html/state_issues.html

Glossary

Clickstreams - In Web advertising, a click stream is the sequence of clicks or pages requested as a visitor explores a Web site.[1]

Cookies – Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user previously or anything about your previous visits. A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer.[2]

Data Matching – Data matching is a process where multiple databases are merged together using a common identifier like a social security number. This allows the company or direct marketer to learn more about the consumer's hobbies, habits, interests and lifestyle, and market their product accordingly. The marketer then sends customized advertisements and coupons to the consumer according to their data.

Data Mining – A class of database applications that look for hidden patterns in a group of data. For example, data mining software can help retail companies find customers with common interests. The term is commonly misused to describe software that presents data in new ways. True data mining software does not just change the presentation, but actually discovers previously unknown relationships among the data.[3]

Electronic commerce (E-commerce; EC) – The use of communication technologies to transmit business information and transact business. Taking an order over the telephone is a simple form of EC. Internet commerce is also EC, but is only one of several advanced forms of EC that use technology integrated applications and business processes to link enterprises.[4]

Electronic government (e-government) – Government activities that takes place by digital processes over a computer network, usually the Internet, between the government and members of the public and entities in the private sector, especially regulated entities. These activities generally involve the electronic exchange of information to acquire or provide products or services, to place or receive orders, to provide or obtain information, or to complete financial transactions. The anticipated benefits of e-government include reduced operating costs for government institutions and regulated entities, increased availability since government services can be accessed from virtually any location, and convenience due to round-the-clock availability. In addition, electronic government provides direct communications between legislators and their constituents via e-mail.

E-mail – Electronic form of communication that allows one to both send message to and receive messages from anyone whom has an e-mail account.

Electronic signatures – An electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.[5]

The **Internet**, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANet.[6]

---

[1] http://www.whatis.com/
[2] http://www.whatis.com/
[3] http://webopedia.internet.com/TERM/d/data_mining.html
[4] Harris, K. "E-Business Glossary: Version 1.0." COM-09-3988. The GartnerGroup. 8 October 1999.
[5] Electronic Signatures in Global and National Commerce Act., Pub. L. S.761, 106th Cong. (2000).
[6] http://www.whatis.com/

Internet Protocol (IP) - The IP part of TCP/IP; the protocol used to route a data packet from its source to its destination over the Internet.[7]

Internet Service Provider (ISP) - A company that provides individuals and other companies access to the Internet and other related services such as Web site building and hosting. An ISP has the equipment and the telecommunication line access required to have points-of-presence on the Internet for the geographic area served. The larger ISPs have their own high-speed leased lines so that they are less dependent on the telecommunication providers and can provide better service to their customers.[8]

Online chat – Real-time communication between two users via computer. Once a chat has been initiated, either user can enter text by typing on the keyboard and the entered text will appear on the other user's monitor.

Opt-in – The Opt-in approach to data release leaves the burden of protection on the business or governmental entity. The subject of the information must give the organization the permission to use their data for other than the original purpose. If such permission is not given, the organization cannot release the subject's data to third parties or use it for purposes other than what it was intended.

Opt-out - The opt-out approach to personal privacy leaves the burden of protection on the subject of the information. The subject has to inform the organization that they do not want their information shared with third parties. If the subject does not give such notice to the organization, the organization reserves the right to share and sell the subject's data.

Personal Information – Personal information can refer to a variety of data, including but not restricted to, one's name, address, telephone, tax history, social security number, credit card number, education, and credit history.

Portal – A high traffic, broadly appealing Web site with a wide range of content, services and vendor links. It acts as a value-added middleman by selecting the content sources and assembling them together in a simple-to-navigate and customize interface for presentation to the end user. Portals typically include services such as e-mail, community and chat.[9]

Privacy policy – A web page that states how the site uses personally identifiable data collected from visitors. Most privacy policies discuss what information is collected, how it is used, and whether it is shared with others.

Web bugs - Web bugs are codes that can identify a particular computer and help advertising services far removed from the site determine whether electronic promotions are well-read and effective in prompting someone to buy a product. They often work with cookies to greatly enhance the ability of outside observers to track and analyze activity, most often without a computer user's knowledge.

Web site - A Web site is a related collection of files that includes a beginning file called a home page. A company or an individual tells you how to get to their Web site by giving you the address of their home page. From the home page, you can get to all the other pages on their site.[10]

World Wide Web - Usually referred to as the "Web," is all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).[11] Pages on the Web can contain graphics, text, audio, and video.

---

[7] http://www.computeruser.com/resources/dictionary/index.html
[8] http://www.whatis.com/
[9] Harris, K. "E-Business Glossary: Version 1.0." COM-09-3988. The GartnerGroup. 8 October 1999.
[10] http://www.whatis.com/
[11] http://www.whatis.com/

Endnotes

[1] Davis, Mary Alice. "Privacy Protection in Texas? Not Yet." Austin American Statesman. 12 January 2000.

[2] Texas Office of the Attorney General. Public Information Handbook 2000.

[3] Texas Office of the Attorney General. Public Information Handbook 2000. Sec Texas Attorney General ORD – 478 (1987).

[4] Associated Credit Bureaus, Inc., *The Market at a Glance*, 1998.

[5] Strover, Sharon and Joe Straubhaar. "E-Government Services and Computer and Internet Use in Texas." Telecommunications and Information Policy Institute. University of Texas at Austin. Commissioned by the Electronic Government Task Force. June, 2000.

[6] Texas. Office of the Attorney General. Texas Public Information Handbook 2000.

[7] Texas. Department of Information Resources. Texas Connected. Service at the Speed of Light. State Strategic Plan for Information Resources Management (1999).

[8] Texas. Department of Information Resources. Texas Connected. Service at the Speed of Light. State Strategic Plan for Information Resources Management (1999).

[9] Washington. Governor's Work Group on Commercial Access to Government Electronic Records. Retrieved on 23 June 2000 from http://www.wa.gov:80/dis/commaccess/es.htm.

Washington. Executive Order 97-01. Retrieved on 23 June 2000 from http://www.governor.wa.gov/eo/eoarchive/eo97-01.htm

[10] Wisconsin. Press Release. "Assembly GOP to Protect Personal Privacy." Retrieved on 8 June 2000 from http://www.legis.state.wi.us/assembly/arc/bodyframe_media_releases_huebschprivacy.htm

[11] Strover, Sharon and Joe Straubhaar. "E-Government Services and Computer and Internet Use in Texas." Telecommunications and Information Policy Institute. University of Texas at Austin. Commissioned by the Electronic Government Task Force. June, 2000.

[12] Davis, Mary Alice. "Privacy Protection in Texas? Not Yet." Austin American Statesman. 12 January 2000.

[13] Texas Office of the Attorney General. "Privacy Acts of the States and the Federal Government." Handout.

[14] Legislating Privacy: Technology, Social Values, and Public Policy. University of North Carolina, Chapel Hill:1995.
The Center of Democracy and Technology, http://www.cdt.org
CNN, http://www.cnn.com
The White House, http://www.whitehouse.gov.

[15] Matthews, William. "Access denied." Federal Computer Week. Retrieved on 2 June 2000 from http://www.fcw.com/fcw/articles/2000/0529/cov-access-05-29-00.asp.

[16] Banisar, David and Simon Davies. "Privacy and Human Rights: International Survey of Privacy Laws and Practice." Privacy International and Electronic Privacy Information Center. Retrieved on 24 March 2000 from http://www.gilc.org/privacy/survey/intro.html.

[17] Banisar, David and Simon Davies. "Privacy and Human Rights: International Survey of Privacy Laws and Practice." Privacy International and Electronic Privacy Information Center. Retrieved on 24 March 2000 from http://www.gilc.org/privacy/survey/intro.html.

[18] Australia. "Privacy: About the Privacy Commissioner." Retrieved on 15 June 2000 from http://www.privacy.gov.au/about/index.html.

[19] Canada. "The Privacy Act – A Preamble." Retrieved on 6 July 2000 from http://www.privcom.gc.ca/english/02_07_e.htm

[20] Canada. "Privacy provision highlights." Department of Justice. Retrieved on 7 July 2000 from http://canada.justice.gc.ca/en/news/nr/1998/attback2.html.

[21] Ontario, Canada. Office of the Information and Privacy Commissioner. Retrieved on 15 June 2000 from http://www.ipc.on.ca/.

[22] Dodd, Jeff. "Privacy Around the World." Smart Computing Guide to PC Privacy. Vol.8 Issue 4, pg.12.

[23] Hong Kong. "Privacy Commissioner's Office – The Ordinance at a Glance. Retrieved on 6 July 2000 from http://www.pco.org.hk/ord/index.html.

[24] Dodd, Jeff. "Us vs. Them: How U.S. Privacy Concerns Compare with Rest of World." Smart Computing Guide to PC Privacy. Vol.8 Issue 4, pg.10-11.

[25] Dodd, Jeff. "Us vs. Them: How U.S. Privacy Concerns Compare with Rest of World." Smart Computing Guide to PC Privacy. Vol.8 Issue 4, pg.12.

[26] "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy." Electronic Privacy Information Center and Junkbusters. June 2000. Retrieved from www.epic.org/reports/prettypoorprivacy.html.

[27] Federal Trade Commission. "Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress." May 2000.

[28] Hoffman, Donna L. and Thomas P. Novak. "How to Acquire Customers on the Web." Harvard Business Review. May-June 2000. Pg. 179.

[29] "The NAMED." Retrieved on 14 April 2000 from http://named.org/why.html.

[30] Meehan, Michael. "E-Commerce CEOs Urge Others to Take Consumer Privacy More Seriously." Computerworld. 16 May 2000.

[31] Meehan, Michael. "E-Commerce CEOs Urge Others to Take Consumer Privacy More Seriously." Computerworld. 16 May 2000.

[32] "Business Group Takes on Privacy." Informationweek.com 10 April 2000.

[33] Foust, Jeff. "MIT Tech Review: Protecting Your Privacy Online." ABCNews.com. Retrieved on 12 May 2000 from http://more.abcnews.go.com/sections/tech/mittechreview/techreview000316.html.

[34] Simons, John. "The Coming Privacy Divide." CNN. 24 February 2000. Retrieved on 17 March 2000 from www.cnn.com/2000/TECH/computing/02/24/privacy.divide.idg/index.html.

[35] Federal Trade Commission. "Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress." May 2000.

[36] Canada. Privacy Commissioner of Canada. "Our Mission and Mandate." Retrieved on 6 July 2000 from http://www.privcom.gc.ca/english/02_01_e.htm.

[37] Ontario, Canada. Our Role: About the Commissioner. Retrieved on 3 August 2000 from http://www.ipc.on.ca/english/our_role/Our_role.htm.

[38] Ontario, Canada. "A Mini Guide to Ontario's Freedom of Information and Protection of Privacy Act." Retrieved on 15 June 2000 from http://www.ipc.on.ca/english/acts/pocket/mini-p.htm.

[40]Hong Kong. "Privacy Commissioner's Office – The Ordinance at a Glance." Retrieved on 6 July 2000 from http://www.pco.org.hk/ord/ord_a.html.

[41] New Zealand. Office of the Privacy Commissioner. "Reception Desk: Meet the Privacy Act, the Commissioner & the Office." Retrieved on 6 July 2000 from http://www.privacy.org.nz/recept/rectop.html.